Discrete Mathematics 22 (1978) 97–98.

NOTE

ON THE EXISTENCE OF A CYCLIC CODE WITH RATE R *

Henk VAN TILBORG

Department of Mathematics, Technological University of Eindhoven, Eindhoven, The Netherlands

Received 18 October 1976
Revised 10 January 1977

In this paper a short proof is given of the existence of a cyclic, q-ary code with rate R, for any rational number R, $0 \leq R \leq 1$.

Coding theorists sometimes need the fact (e.g. in [1]) that the rates of cyclic codes are dense in the interval [0, 1]. A natural question that arises is: Given a rational R, $0 \leq R \leq 1$, does there exist a cyclic, q-ary (n, k) code, with $R = k/n$. The answer is affirmative as we shall now show.

Let K_q be defined by

$$K_q := \{k/n : \text{there exists a } q\text{-ary, cyclic } (n, k) \text{ code}\}.$$

Lemma 1. *The set K_q has the following properties*

(1) $0 \in K_q$, $1 \in K_q$,
(2) $1/n \in K_q$ *for any integer* $n \geq 1$,
(3) $k/n \in K_q \Rightarrow (n-k)/n \in K_q$,
(4) $k/n \in K \Rightarrow k/mn \in K_q$ *for any integer* $m \geq 1$.

Proof. Property (1) is obvious. The existence of a q-ary, cyclic (n, k) code is equivalent to the existence of a q-ary polynomial $g(x)$ of degree $n-k$, dividing $x^n - 1$. So properties (2), (3), and (4) follow from the following observations:

(a) $(x-1) \mid (x^n - 1)$,
(b) $g(x) \mid (x^n - 1) \Rightarrow (x^n - 1)/g(x) \mid (x^n - 1)$,
(c) $g(x) \mid (x^n - 1) \Rightarrow g(x) \mid (x^{nm} - 1)$.

Theorem 2. $K_q = \{0 \leq r \leq 1 : r \text{ rational}\}$.

* The work was done while the author was with the Department of Mathematics at Caltech and represents one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology under Contract NAS 7-100, sponsored by the National Aeronautics and Space Administration.

Proof. Let $n \in \mathbf{N}$. We shall show that for any k with $0 \leq k \leq n$, $k/n \in K_q$. The proof is by induction on k. By properties (1) and (2) of Lemma 1, $0/n \in K_q$ and $1/n \in K_q$. Now suppose that we have proved that $k/n \in K_q$, for $0 \leq k \leq r$ $(r \geq 1)$. We need to show that $(r+1)/n \in K_q$. Let

$$n = a(r+1)+s, \qquad 0 \leq s \leq r.$$

Since $s \leq r$, $s/n \in K_q$ and by property (3), $(n-s)/n \in K_q$. Now

$$\frac{r+1}{n} = \frac{a(r+1)}{an} = \frac{n-s}{an} = \frac{1}{a} \cdot \frac{n-s}{n} \in K_q,$$

by property (4) of Lemma 1.

Reference

[1] R.J. McEliece and A.L. Rubin, Timesharing without synchronization, Proc. 1976 International Telemetering Conference (Instrument Society of America) 16–20.